

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-88431

(43) 公開日 平成11年(1999) 3月30日

(51) Int.Cl.<sup>5</sup>

識別記号

F I

H 0 4 L 12/56

H 0 4 L 11/20

1 0 2 A

G 0 6 F 13/00

3 5 3

G 0 6 F 13/00

3 5 3 C

H 0 4 B 7/26

G 0 9 C 1/00

6 6 0 E

H 0 4 L 9/14

H 0 4 B 7/26

M

// G 0 9 C 1/00

6 6 0

H 0 4 L 9/00

6 4 1

審査請求 未請求 請求項の数11 O L (全 19 頁)

(21) 出願番号

特願平9-241156

(22) 出願日

平成9年(1997) 9月5日

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 井上 淳

神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

(72) 発明者 石山 政浩

神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

(72) 発明者 福本 淳

神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

(74) 代理人 弁理士 鈴江 武彦 (外6名)

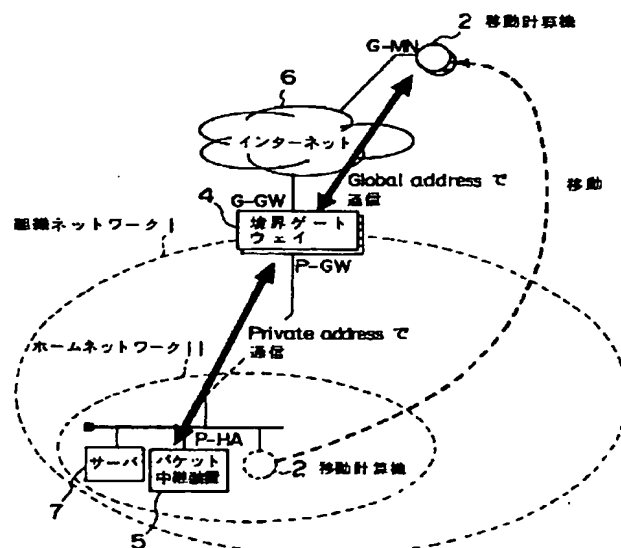
最終頁に続く

(54) 【発明の名称】 パケット中継装置、移動計算機装置、移動計算機管理装置、パケット中継方法、パケット送信方法及び移動計算機位置登録方法

(57) 【要約】

【課題】 移動計算機が組織外のグローバルアドレスに移動しても移動IP方式をそのまま使用し続けること可能とするパケット中継装置を提供すること。

【解決手段】 ホームエージェントの属するネットワーク内に設置され、ネットワーク内との通信では内部アドレスを外部との通信では外部アドレスを用い、ネットワーク外に移動した計算機から自身の外部アドレス宛の暗号化パケットを受信し復号して得た内部パケットの宛先計算機宛に、内部パケットを再度暗号化し送信元を自装置の内部アドレス、宛先を宛先計算機のアドレスとするヘッダを付加したパケットを転送し、ネットワーク内の計算機から自身の内部アドレス宛の暗号化パケットを受信し復号して得た内部パケットの宛先移動計算機宛に、内部パケットを再度暗号化し送信元を自装置の外部アドレス、宛先を移動計算機の現在位置アドレスとするヘッダを付加したパケットを転送する。



## 【特許請求の範囲】

【請求項 1】 ネットワーク間を移動して通信を行うことが可能な移動計算機の移動位置情報を管理し、該移動計算機宛のバケットを該移動計算機の現在位置アドレス宛に転送する手段を有する移動計算機管理装置の設置されたネットワーク内に設置された、ネットワーク内に位置する計算機とネットワーク外に位置する計算機との間で送受信されるバケットを中継するバケット中継装置であって、

前記ネットワーク内部の計算機との間での通信に用いる内部アドレスと、前記ネットワーク外部の計算機との間での通信に用いる外部アドレスとを記憶する第 1 の記憶手段と、

前記ネットワーク内部に属する各移動計算機の所属アドレス情報、各移動計算機が前記ネットワーク外部に移動した場合の現在位置アドレス情報、および前記ネットワーク外部に移動した各移動計算機との間でのバケット暗号化のための鍵情報を少なくとも対応付けて記憶する第 2 の記憶手段と、

前記ネットワーク外部に移動した移動計算機から送信された暗号化バケットを対応する前記鍵情報を用いて復号し、得られた内部バケットの宛先となる計算機宛に、該内部バケットを再度暗号化し、さらに送信元を自装置の内部アドレス、宛先を該宛先計算機のアドレスとするヘッダを付加して得たバケットを転送する手段と、

前記ネットワーク内部の計算機から送信された暗号化バケットを復号し、得られた内部バケットの宛先となる移動計算機に対応する前記鍵情報で該内部バケットを再度暗号化し、さらに送信元を自装置の外部アドレス、宛先を該移動計算機の現在位置アドレスとするヘッダを付加して、該移動計算機に転送する手段とを備えたことを特徴とするバケット中継装置。

【請求項 2】 前記ネットワーク外部に移動した移動計算機から送信された暗号化バケットを復号して得た前記内部バケットが、前記移動計算機管理装置宛の現在移動アドレス情報を含む登録要求バケットである場合、該現在移動アドレス情報を前記第 2 の記憶手段に登録する手段をさらに備えたことを特徴とする請求項 1 に記載のバケット中継装置。

【請求項 3】 相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置であって、自装置の移動位置情報を管理し自装置宛のバケットを自装置の現在位置アドレス宛に転送する移動計算機管理装置宛に直接バケットを送信することが可能な、該移動計算機管理装置の設置されたネットワークと同じアドレス空間に自装置が接続しているか否かを示す情報を記憶する手段と、

自装置を対象とする前記移動計算機管理装置の設置されたネットワークと異なるアドレス空間と、該ネットワークと同じアドレス空間との境界に設置され、アドレス空

間ごとに設定されたアドレスを用いて、両アドレス空間にそれぞれ接続された計算機間で送受信されるバケットを中継するバケット中継装置の、該異なるアドレス空間におけるアドレスを記憶する手段と、

自装置が前記移動計算機管理装置の設置されたネットワークと異なるアドレス空間に接続していることを示す情報が記憶されている場合、該移動計算機管理装置宛の現在移動アドレス情報を含む登録要求バケットを、前記バケット中継装置宛に暗号化して送信する手段とを備えたことを特徴とする移動計算機装置。

【請求項 4】 相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置であって、自装置の移動位置情報を管理し自装置宛のバケットを自装置の現在位置アドレス宛に転送する移動計算機管理装置宛に直接バケットを送信することが可能な、該移動計算機管理装置の設置されたネットワークと同じアドレス空間に、自装置が接続しているか否かを示す情報を記憶する手段と、

自装置を対象とする前記移動計算機管理装置の設置されたネットワークと異なるアドレス空間と、該ネットワークと同じアドレス空間との境界に設置され、アドレス空間ごとに設定されたアドレスを用いて、両アドレス空間にそれぞれ接続された計算機間で送受信されるバケットを中継するバケット中継装置の、該異なるアドレス空間におけるアドレスを記憶する手段と、

自装置が前記移動計算機管理装置の設置されたネットワークと異なるアドレス空間に接続していることを示す情報が記憶されている場合、該ネットワーク内に位置する計算機を宛先とするバケット全体を暗号化して前記バケット中継装置宛に送信する手段とを備えたことを特徴とする移動計算機装置。

【請求項 5】 移動先におけるアドレスを自動取得するか否かを設定する手段と、

自装置が前記移動計算機管理装置の設置されたネットワークと異なるアドレス空間に接続していることを示す前記設定がされている場合に、前記アドレスを自動取得することを示す設定がされているならば、アドレスの割当てを受けるための所定のプロトコルを実行して取得したアドレスを自装置の現在位置アドレスとする手段とをさらに備えたことを特徴とする請求項 3 または 4 に記載の移動計算機装置。

【請求項 6】 ネットワーク間を移動して通信を行うことが可能な移動計算機の移動位置情報を管理し、該移動計算機宛のバケットを該移動計算機の現在位置に転送する手段を有するバケット中継装置であって、自装置の属するネットワーク内部に属する各移動計算機の所属アドレス情報および各移動計算機が該ネットワーク外部に移動した場合の現在位置アドレス情報を少なくとも対応付けて記憶する記憶手段と、

自装置の属するネットワークと同じアドレス空間と、該

3

アドレス空間とは異なるアドレス空間との境界に設置され、アドレス空間ごとに設定されたアドレスを用いて、両アドレス空間にそれぞれ接続された計算機間で送受信されるパケットを中継するパケット中継装置から中継されてきた暗号化パケットを復号し、得られた内部パケットが自装置の管理対象とする移動計算機から自装置宛に発せられた現在移動アドレス情報を含む登録要求パケットである場合、該現在移動アドレス情報を前記記憶手段に登録する手段とを備えたことを特徴とするパケット中継装置。

【請求項 7】前記登録要求パケットに対する前記移動計算機宛の登録応答パケットを、前記パケット中継装置宛に暗号化して送信する手段をさらに備えたことを特徴とする請求項 6 に記載のパケット中継装置。

【請求項 8】自装置の属するネットワーク外部に移動中の移動計算機の前記所属アドレス宛に転送されてきたパケットを捕捉した場合、該パケットを、送信元を自装置のアドレス、宛先を該移動計算機の該所属アドレスとするパケットにカプセル化した後に、さらにこのカプセル化されたパケットを、前記パケット中継装置宛に暗号化して送信する手段をさらに備えたことを特徴とする請求項 6 または 7 に記載のパケット中継装置。

【請求項 9】ネットワーク間を移動して通信を行うことが可能な移動計算機の移動位置情報を管理し、該移動計算機宛のパケットを該移動計算機の現在位置アドレス宛に転送する手段を有する移動計算機管理装置の設置されたネットワーク内に設置された、ネットワーク内に位置する計算機とネットワーク外に位置する計算機との間で送受信されるパケットを中継するとともに、該ネットワーク内部の計算機との間での通信には内部アドレスを用い、該ネットワーク外部の計算機との間での通信には外部アドレスを用いるパケット中継装置におけるパケット中継方法であって、

前記ネットワーク外部に移動した移動計算機から自装置の外部アドレス宛に送信された暗号化パケットを受信した場合、この暗号化パケットを対応する鍵情報を用いて復号し、得られた内部パケットの宛先となる計算機宛に、該内部パケットを再度暗号化し、さらに送信元を自装置の内部アドレス、宛先を該宛先計算機のアドレスとするヘッダを付加して得たパケットを転送するとともに、

前記ネットワーク内部の計算機から自装置の内部アドレス宛に送信された暗号化パケットを受信した場合、該暗号化パケットを復号し、得られた内部パケットの宛先となる移動計算機に対応する鍵情報で該内部パケットを再度暗号化し、さらに送信元を自装置の外部アドレス、宛先を該移動計算機の現在位置アドレスとするヘッダを付加して、該移動計算機に転送する手段とを備えたことを特徴とするパケット中継方法。

【請求項 10】相互に接続されたネットワーク間を移動

4

して通信を行うことが可能な移動計算機装置におけるパケット送信方法であって、

自装置の移動位置情報を管理し自装置宛のパケットを自装置の現在位置アドレス宛に転送する移動計算機管理装置の属するネットワーク内に位置する計算機を宛先とするパケットを送信する場合、該移動計算機管理装置の設置されたネットワークと同じアドレス空間に自装置が接続されていないことを示す情報が設定されているならば、

10 自装置を対象とする前記移動計算機管理装置の設置されたネットワークと異なるアドレス空間と、該ネットワークと同じアドレス空間との境界に設置され、アドレス空間ごとに設定されたアドレスを用いて、両アドレス空間にそれぞれ接続された計算機間で送受信されるパケットを中継するパケット中継装置の、該異なるアドレス空間におけるアドレス宛に、該ネットワークにおける自装置および宛先計算機のアドレスを含むパケット全体を暗号化して送信することを特徴とするパケット送信方法。

20 【請求項 11】ネットワーク間を移動して通信を行うことが可能な移動計算機の移動位置情報を管理し、該移動計算機宛のパケットを該移動計算機の現在位置に転送する手段を有するパケット中継装置における移動計算機登録方法であって、

自装置の属するネットワークと同じアドレス空間と、該アドレス空間とは異なるアドレス空間との境界に設置され、アドレス空間ごとに設定されたアドレスを用いて、両アドレス空間にそれぞれ接続された計算機間で送受信されるパケットを中継するパケット中継装置から中継されてきた暗号化パケットを受信した場合、該暗号化パケットを復号し、

30 得られた内部パケットが自装置の管理対象とする移動計算機から自装置宛に発せられた現在移動アドレス情報を含む登録要求パケットである場合、該現在移動アドレス情報を登録することを特徴とする移動計算機登録方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、相互接続している複数のネットワーク上を移動しながら通信を行う移動計算機及びその移動計算機を宛先または送信元とするデータパケットを中継するパケット中継装置並びにパケット中継方法、パケット送信方法及び移動計算機登録方法に関する。

【0002】

【従来の技術】計算機システムの小型化、低価格化やネットワーク環境の充実に伴って、計算機システムの利用は急速にかつ種々の分野に広く拡大し、また集中型システムから分散型システムへの移行が進んでいる。特に近年では計算機システム自体の進歩、能力向上に加え、コンピュータ・ネットワーク技術の発達・普及により、オフィス内のファイルやプリンタなどの資源共有のみなら

50

5  
ず、オフィス外、一組織外とのコミュニケーション（電子メール、電子ニュース、ファイルの転送など）が可能になり、これらが広く利用されはじめた。特に近年では、世界最大のコンピュータネットワーク「インターネット（internet）」の利用が普及しており、インターネットと接続し、公開された情報、サービスを利用したり、逆にインターネットを通してアクセスしてくる外部ユーザに対し、情報、サービスを提供すること  
で、新たなコンピュータビジネスが開拓されている。また、インターネット利用に関して、新たな技術開発、展開がなされている。

開がなされている。

【0003】また、このようなネットワークの普及に伴い、移動通信 (mobile computing) に対する技術開発も行われている。移動通信では、携帯型端末、計算機を持ったユーザがネットワーク上を移動して通信する。ときには通信を行いながらネットワーク上の位置を変えていく場合もあり、そのような通信において変化する移動計算機のネットワーク上を管理し、正しく通信内容を到達させるための方式が必要である。

しく通信内容を到達させるための方式が必要である。

【0004】一般に移動通信を行う場合、移動計算機が 20  
所属していたネットワークに移動計算機の移動先データ  
を管理するルータ（ホームエージェント）を置き、移動  
計算機が移動した場合、このホームエージェントに対し  
て現在位置を示す登録メッセージを送る。登録メッセ  
ジが受け取られたら、移動計算機宛データの送信はその  
ホームエージェントを経由して、移動計算機の元のアド  
レス宛の IP パケットを移動計算機の現在位置アドレ  
ス宛のパケット内にカプセル化することで移動計算機に対す  
るデータの経路制御が行われる。例えば、図 6 では、元  
々ホームネットワーク 101a に属していた移動計算機 30  
102 が、他のネットワーク 101b に移動し、ネット  
ワーク 101c 内の他の計算機（CH）103 との間で  
通信を行う場合に、移動計算機 102 に対しホームエ  
ージェント（HA）105 が上記の役割を行う。この方式  
は、インターネットの標準化団体である IETF の mo  
bile-IP ワーキンググループで標準化が進められ  
ている移動 IP と呼ばれる方式である（文献：RFC 2  
002, IP mobility support  
(C. Perkins)）。

(C. Perkins) )。 40  
【0005】また、ネットワークが普及し、ネット間の自由な接続が実現され、膨大なデータ、サービスのやりとりがなされる場合、セキュリティ上の問題を考慮する必要がある。例えば組織内部の秘密情報の外部ネットワークへの漏洩をいかに防ぐか、という問題や、組織外からの不正な侵入から、組織内ネットワークに接続された資源、情報をいかに守るか、という問題である。インターネットは、当初学術研究を目的に構築されたため、ネットワークの接続による自由なデータサービスのやりとりを重視しており、このようなセキュリティ上の問題は考慮されていなかったが、近年多くの企業、団体

がインターネットに接続できるようになり、セキュリティ上の問題から自組織ネットワークを防衛する機構が必要となってきた。

となってきた。  
【0006】そこで、インターネット上でデータパケットを交換する際に、外部にデータパケットを送出する前にその内容を暗号化し認証コードをつけ、受信したサイトで認証コードを確認し復号化する、という方法がある。この方法によれば、たとえ組織外のユーザが外部ネットワーク上のデータパケットを取り出しても、内容が暗号化されているので、決してその内部が漏洩することがなく、安全な通信が確保できる。

がなく、安全な通信が確保できる。

【0007】このような暗号化通信をサポートするゲートウェイ計算機で守られた（ガードされた）ネットワーク同士であれば相互に暗号化通信が可能であり、また前述の移動計算機が自分でパケットの暗号化、復号を行う機能をサポートしていれば、任意のゲートウェイ間、またはゲートウェイ～移動計算機間で暗号化通信をサポートできる。例えば図6では、元々ホームネットワーク101aに属していた移動計算機102が、他のネットワーク101bに移動し、ネットワーク101c内の他の計算機（CH）103と暗号化、復号機能をサポートするゲートウェイ104a、104cを介して暗号化通信を行う。

【0008】図6では、移動IPとパケット暗号化を併用して通信を行う場合、パケットの転送経路は、CH→ゲートウェイ104c→ゲートウェイ104a→ホームエージェント(HA)105→ゲートウェイ104a→移動計算機102となり、ゲートウェイ104aでは、一旦パケットは復号化されてホームエージェント105に送られ、その後、再度ホームエージェント105発のパケットが暗号化される。

【0009】さて、移動IP方式では、単一のアドレス空間上を移動計算機が移動する場合のみを想定して、プロトコルが構成されている。すなわち、移動先からの現在位置の登録メッセージは必ずホームネットのホームエージェントに到達可能であると仮定している。しかし、昨今では大規模な組織がインターネットに接続する場合、IPアドレスの枯渇の問題から、組織内の全てのホストにグローバルIPアドレスが割り当てられているのは稀で、組織内はプライベートアドレス（文献：RFC 1597）で運用し、外部に通信する場合は、グローバルアドレスへのアドレス変換を行う場合が多い。

【0010】その場合、グローバルアドレス領域に移動した移動計算機から、プライベートアドレス領域内のホームエージェントに送信された登録要求パケットは、そのまきでは到達可能でない。

【0011】そこで、このような複数のアドレス空間が混在するネットワーク構成では、組織ネットワークの入口で移動計算機から送信された登録要求パケットを一旦

受信し、内容を確認して、組織内の該当するホームエージェント宛に転送する処理が必要である（移動IP方式では、ホームエージェントはサブネットに1つ設置されるので、組織内に複数のホームエージェントが置かれることがあるため）。また、移動計算機の側でも、自分がプライベートアドレス領域で移動しているのか、グローバルアドレス領域に移動したかに応じて、登録要求パケットの内容を変える制御機構が必要になる。

【0012】以上説明したように、一般に移動IP方式を利用して移動計算機をサポートする場合、移動計算機が複数のアドレス空間に渡って移動（プライベート→グローバルのように）する場合、移動計算機の現在位置に応じホームネットのホームエージェント宛に送信する登録要求などのパケット形式を制御するための方式や、プライベートネット／グローバルネットの境界である組織入口で、送信されたパケットを一旦受信し、内容を確認して、組織内の該当するホームエージェント宛に転送するための方式が必要になる。

#### 【0013】

【発明が解決しようとする課題】従来の移動IP方式では、移動計算機はホームネットワークとの到達可能性（reachability）を仮定してプロトコルを構成していたため、ホームネットワークと共通のアドレス空間内のみを移動するという制約があった。このため、組織がプライベートアドレスで運用された場合、移動計算機が組織ネットワークの外（グローバルアドレス領域）に移動すると、移動IP方式がそのまま使用できないという欠点があった。

【0014】本発明は、上記事情を考慮してなされたもので、複数の計算機が複数の相互接続された通信ネットワークにより互いに接続されて相互に通信可能に構成された計算機システムで、移動IPによる移動計算機への自動経路制御がサポートされている場合において、ホームネットワークと異なるアドレス管理領域に移動した移動計算機発の位置登録メッセージなどのパケットを、組織ネットワークの入口で一旦受信し、内容を確認して、組織内の該当するホームエージェント宛に転送する処理を行うと共に、移動計算機側でも自身の現在位置に応じて適切な形式でパケットを生成、送信するような移動計算機制御を可能とするパケット中継装置、移動計算機装置、パケット中継方法、パケット送信方法及び移動計算機登録方法を提供することを目的とする。

#### 【0015】

【課題を解決するための手段】本発明（請求項1）は、ネットワーク間を移動して通信を行うことが可能な移動計算機の移動位置情報を管理し、該移動計算機宛のパケットを該移動計算機の現在位置アドレス宛に転送する手段を有する移動計算機管理装置（ホームエージェント、実施形態におけるパケット中継装置）の設置されたネットワーク内に設置された、ネットワーク内に位置する計

算機（前記移動計算機管理装置も含む）とネットワーク外に位置する計算機（前記移動計算機も含む）との間で送受信されるパケットを中継するパケット中継装置（境界ゲートウェイ）であって、前記ネットワーク内部の計算機との間での通信に用いる内部アドレス（例えばプライベートアドレス）と、前記ネットワーク外部の計算機との間での通信に用いる外部アドレス（例えばグローバルアドレス）とを記憶する第1の記憶手段と、前記ネットワーク内部に属する各移動計算機の所属アドレス情報、各移動計算機が前記ネットワーク外部に移動した場合の現在位置アドレス情報、および前記ネットワーク外部に移動した各移動計算機との間でのパケット暗号化のための鍵情報を少なくとも対応付けて記憶する第2の記憶手段と、前記ネットワーク外部に移動した移動計算機から送信された暗号化パケットを対応する前記鍵情報を用いて復号し、得られた内部パケット（登録要求パケットも含む）の宛先となる計算機宛に、該内部パケットを再度暗号化し、さらに送信元を自装置の内部アドレス、宛先を該宛先計算機のアドレスとするヘッダを付加して得たパケットを転送する手段と、前記ネットワーク内部の計算機（前記移動計算機管理装置も含む）から送信された暗号化パケットを復号し、得られた内部パケット（登録応答パケットも含む）の宛先となる移動計算機に

対応する前記鍵情報で該内部パケットを再度暗号化し、さらに送信元を自装置の外部アドレス、宛先を該移動計算機の現在位置アドレスとするヘッダを付加して、該移動計算機に転送する手段とを備えたことを特徴とする。

【0016】好ましくは、前記ネットワーク外部に移動した移動計算機から送信された暗号化パケットを復号して得た前記内部パケットが、前記移動計算機管理装置宛の現在移動アドレス情報を含む登録要求パケットである場合、該現在移動アドレス情報を前記第2の記憶手段に登録する手段をさらに備えるようにしてもよい。

【0017】本発明（請求項3）は、相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置であって、自装置の移動位置情報を管理し自装置宛のパケットを自装置の現在位置アドレス宛に転送する移動計算機管理装置（ホームエージェント、実施形態におけるパケット中継装置）宛に直接パケットを送信することが可能な、該移動計算機管理装置の設置されたネットワークと同じアドレス（例えばプライベートアドレス）空間に自装置が接続しているか否かを示す情報を記憶する手段と、自装置を対象とする前記移動計算機管理装置の設置されたネットワークと異なるアドレス（例えばグローバルアドレス）空間と、該ネットワークと同じアドレス空間との境界に設置され、アドレス空間ごとに設定されたアドレスを用いて、両アドレス空間にそれぞれ接続された計算機（前記移動計算機、前記移動計算機管理装置も含む）間で送受信されるパケットを中継するパケット中継装置（境界ゲートウェイ）の、該異なる

10

20

30

40

50

アドレス空間におけるアドレスを記憶する手段と、自装置が前記移動計算機管理装置の設置されたネットワークと異なるアドレス空間に接続していることを示す情報が記憶されている場合、該移動計算機管理装置宛の現在移動アドレス情報を含む登録要求パケットを、前記パケット中継装置宛に暗号化して送信する手段とを備えたことを特徴とする。

【0018】本発明（請求項4）は、相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置であって、自装置の移動位置情報を管理し自装置宛のパケットを自装置の現在位置アドレス宛に転送する移動計算機管理装置宛に直接パケットを送信することが可能な、該移動計算機管理装置（ホームエージェント、実施形態におけるパケット中継装置）の設置されたネットワークと同じアドレス（例えばプライベートアドレス）空間に、自装置が接続しているか否かを示す情報を記憶する手段と、自装置を対象とする前記移動計算機管理装置の設置されたネットワークと異なるアドレス（例えばグローバルアドレス）空間と、該ネットワークと同じアドレス空間との境界に設置され、アドレス空間ごとに設定されたアドレスを用いて、両アドレス空間にそれぞれ接続された計算機（前記移動計算機、前記移動計算機管理装置も含む）間で送受信されるパケットを中継するパケット中継装置（境界ゲートウェイ）の、該異なるアドレス空間におけるアドレスを記憶する手段と、自装置が前記移動計算機管理装置の設置されたネットワークと異なるアドレス空間に接続していることを示す情報が記憶されている場合、該ネットワーク内に位置する計算機を宛先とするパケット全体を暗号化して前記パケット中継装置宛に送信する手段とを備えたことを特徴とする。

【0019】好ましくは、移動先におけるアドレスを自動取得するか否かを設定する手段と、自装置が前記移動計算機管理装置の設置されたネットワークと異なるアドレス空間に接続していることを示す前記設定がされている場合に、前記アドレスを自動取得することを示す設定がされているならば、アドレスの割当てを受けるための所定のプロトコル（例えばPPPプロトコル）を実行して取得したアドレスを自装置の現在位置アドレスとする手段とをさらに備えるようにしてもよい。

【0020】本発明（請求項6）は、ネットワーク間を移動して通信を行うことが可能な移動計算機の移動位置情報を管理し、該移動計算機宛のパケットを該移動計算機の現在位置に転送する手段を有するパケット中継装置（実施形態におけるパケット中継装置）であって、自装置の属するネットワーク内部に属する各移動計算機の所属アドレス情報および各移動計算機が該ネットワーク外部に移動した場合の現在位置アドレス情報を少なくとも対応付けて記憶する記憶手段と、自装置の属するネットワークと同じアドレス（例えばプライベートアドレス）

空間と、該アドレス空間とは異なるアドレス（例えばグローバルアドレス）空間との境界に設置され、アドレス空間ごとに設定されたアドレスを用いて、両アドレス空間にそれぞれ接続された計算機（前記移動計算機、前記移動計算機管理装置も含む）間で送受信されるパケットを中継するパケット中継装置（境界ゲートウェイ）から中継されてきた暗号化パケットを復号し、得られた内部パケットが自装置の管理対象とする移動計算機から自装置宛に発せられた現在移動アドレス情報を含む登録要求パケットである場合、該現在移動アドレス情報を前記記憶手段に登録する手段とを備えたことを特徴とする。

【0021】好ましくは、前記登録要求パケットに対する前記移動計算機宛の登録応答パケットを、前記パケット中継装置宛に暗号化して送信する手段をさらに備えるようにしてもよい。

【0022】好ましくは、自装置の属するネットワーク外部に移動中の移動計算機の前記所属アドレス宛に転送されてきたパケットを捕捉した場合、該パケットを、送信元を自装置のアドレス、宛先を該移動計算機の該所属アドレスとするパケットにカプセル化した後に、さらにこのカプセル化されたパケットを、前記パケット中継装置宛に暗号化して送信する手段をさらに備えるようにしてもよい。

【0023】本発明（請求項9）は、ネットワーク間を移動して通信を行うことが可能な移動計算機の移動位置情報を管理し、該移動計算機宛のパケットを該移動計算機の現在位置アドレス宛に転送する手段を有する移動計算機管理装置の設置されたネットワーク内に設置された、ネットワーク内に位置する計算機とネットワーク外に位置する計算機との間で送受信されるパケットを中継するとともに、該ネットワーク内部の計算機との間での通信には内部アドレスを用い、該ネットワーク外部の計算機との間での通信には外部アドレスを用いるパケット中継装置（境界ゲートウェイ）におけるパケット中継方法であって、前記ネットワーク外部に送信された暗号化パケットを受信した場合、この暗号化パケットを対応する鍵情報を用いて復号し、得られた内部パケットの宛先となる計算機宛に、該内部パケットを再度暗号化し、さらに送信元を自装置の内部アドレス、宛先を該宛先計算機のアドレスとするヘッダを付加して得たパケットを転送するとともに、前記ネットワーク内部の計算機から自装置の内部アドレス宛に送信された暗号化パケットを受信した場合、該暗号化パケットを復号し、得られた内部パケットの宛先となる移動計算機に対応する鍵情報で該内部パケットを再度暗号化し、さらに送信元を自装置の外部アドレス、宛先を該移動計算機の現在位置アドレスとするヘッダを付加して、該移動計算機に転送する手段とを備えたことを特徴とする。

【0024】本発明（請求項10）は、相互に接続され

たネットワーク間を移動して通信を行うことが可能な移動計算機装置におけるパケット送信方法であって、自装置の移動位置情報を管理し自装置宛のパケットを自装置の現在位置アドレス宛に転送する移動計算機管理装置の属するネットワーク内に位置する計算機を宛先とするパケットを送信する場合、該移動計算機管理装置の設置されたネットワークと同じアドレス空間に自装置が接続されていないことを示す情報が設定されているならば、自装置を対象とする前記移動計算機管理装置の設置されたネットワークと異なるアドレス空間と、該ネットワークと同じアドレス空間との境界に設置され、アドレス空間ごとに設定されたアドレスを用いて、両アドレス空間にそれぞれ接続された計算機間で送受信されるパケットを中継するパケット中継装置の、該異なるアドレス空間におけるアドレス宛に、該ネットワークにおける自装置および宛先計算機のアドレスを含むパケット全体を暗号化して送信することを特徴とする。

【0025】本発明（請求項11）は、ネットワーク間を移動して通信を行うことが可能な移動計算機の移動位置情報を管理し、該移動計算機宛のパケットを該移動計算機の現在位置に転送する手段を有するパケット中継装置（実施形態におけるパケット中継装置）における移動計算機登録方法であって、自装置の属するネットワークと同じアドレス空間と、該アドレス空間とは異なるアドレス空間との境界に設置され、アドレス空間ごとに設定されたアドレスを用いて、両アドレス空間にそれぞれ接続された計算機間で送受信されるパケットを中継するパケット中継装置から中継されてきた暗号化パケットを受信した場合、該暗号化パケットを復号し、得られた内部パケットが自装置の管理対象とする移動計算機から自装置宛に発せられた現在移動アドレス情報を含む登録要求パケットである場合、該現在移動アドレス情報を登録することを特徴とする。

【0026】なお、以上の各装置に係る発明は方法に係る発明としても成立し、方法に係る発明は装置に係る発明としても成立する。また、上記の発明は、相当する手順あるいは手段をコンピュータに実行させるためのプログラムを記録した機械読取り可能な媒体としても成立する。

【0027】従来、移動IP方式では、移動計算機はホームネットワークとの到達可能性（reachability）の保証された単一空間内でのみ移動が許されており、例えば大規模な組織で組織内ネットワークをプライベートアドレスで構築している場合、組織外のグローバルアドレス領域に移動した計算機からは移動IP方式をそのまま使用できなかった。これに対して本発明によれば、移動計算機側で自身の現在位置に応じて適切な形式でパケットを生成、送信するような制御を可能とし、また、組織ネットワークの入口で移動計算機からのパケットを一旦受信し、内容を確認して、組織内の該当する

パケット中継装置（ホームエージェント）宛に転送する処理を行うことにより、例えば企業ネットがプライベートアドレスで運用しており、移動計算機が組織外のグローバルアドレスに移動しても移動IP方式をそのまま使用し続けることができる。

【0028】一般に、大規模ネットワークでは、企業ネットの入口で通信内容のログを取ったりすることが多く、パケット中継装置（境界ゲートウェイ）の処理のオーバーヘッドは実際には問題にならない場合が多い。また、パケット中継装置（境界ゲートウェイ）でファイアウォールなどの他の制御機構を共存させる場合も拡張が容易である。

【0029】また、本発明において、インターネットプロバイダなどに接続するシーケンス内で移動計算機のIPネットワーク上の位置を検出することで、移動計算機側の制御をさらに容易にできる。

【0030】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。図1に、本実施形態に係るネットワークの基本構成を示す。図1では、組織ネットワーク1の中にホームネットワーク11が存在する。組織ネットワーク（例えば企業内ネットワーク）1全体はプライベートアドレスで運用されている。移動計算機2は、本来、ホームネットワーク11に接続されているが、現在は移動して、組織ネットワーク外のグローバルアドレスで運用されている箇所に接続されているとする。

【0031】ホームネットワーク11には、パケット中継装置5が設置される。このパケット中継装置5は、パケット暗号化の機能と、移動IPのホームエージェントの機能（移動計算機の現在位置を管理し、移動計算機宛に送られてきたパケットをカプセル化して現在位置に転送する機能）とを持っている。

【0032】組織ネットワーク1の出口すなわちインターネット6との境界部分には、境界ゲートウェイ4が設置される。この境界ゲートウェイ4は、2つのインタフェースを持ち、組織外のグローバルアドレス（インターネット側）と組織内のプライベートアドレスの両方を持つ。

【0033】なお、本実施形態ではノード間のデータ転送に暗号化通信を用いるが、このノード間の暗号化通信には、ノード間で共有された該ノード間に固有の共通鍵を用いるものとする。この共通鍵は予めノード間で共有しておくか、あるいは必要時にノード間で鍵共有のための手続きを行う。

【0034】以下では移動計算機2が移動先からホームネットワーク11内のパケット中継装置5との間で移動登録に関するやり取りを行う場合とサーバ7と通信する場合を例にとりつつ本実施形態について詳しく説明する。

【0035】移動計算機2側では、自身の接続している

現在位置に関する情報を図2に例示する制御パネルで設定する。ここで、Private Address Regionは移動計算機2が同じプライベートアドレス体系で運営される組織ネット内で移動したことを、Global Address Regionは組織ネット外部に出たことを示す。

【0036】Global Address Regionを選択した場合は、Border Gateway IP addressに境界ゲートウェイ4のグローバルアドレスを設定する（例えば、202, 249, 10, 122）。また、自身の現在位置のアドレスを設定する（この設定フィールドは図2においては省略してある）。

【0037】なお、上記では、ユーザが陽に指定を行うようにしたが、例えばインターネットプロバイダーのサーバとPPPで接続する際のネゴシエーションメッセージを基にこれらの情報を自動的に設定することも可能である。すなわち、一般にインターネットプロバイダと電話回線を通じてPPPというプロトコルでIP接続を行う場合、PPPプロトコルの初期セット時にICPというプロトコルで割り当てられるアドレスを決める。そのような場合、移動計算機2側では特定のアドレスを設定できないので、例えば図3のように、「アドレスをISP側から自動的に割り当てする」あるいは「アドレスを自動取得する」というような設定ボタンを設け、これを選択する。これを選択した場合、PPPのプロトコルの途上で獲得したIPアドレスがそのまま現在位置アドレスにセットされる。

【0038】次に、図2に例示した制御パネルで（あるいは自動的に）現在位置が設定された場合の移動登録メッセージの送信動作を説明する。まず、プライベートネット内で移動した場合について説明する。

【0039】移動計算機2は、組織内（例えば企業内）のプライベートネット内で移動した旨の情報がセットされると、通常の移動IPの規定通り、ホームネットワーク11の packets 中継装置5宛に、対応する鍵で登録要求 packets のペイロードを暗号化して送信する。

【0040】暗号化された登録要求 packets を受信した packets 中継装置5では、送信元の移動計算機2に対応する鍵で該 packets を復号し、得られた packets の内容を検査する。packets ・ヘッダ内の識別情報（例えば packets タイプ・フィールドに記述されたコード）から移動IPの登録要求であることが判ると、該 packets から該移動計算機2のホームアドレスと現在位置アドレスを取り出し、これを図5のような管理テーブルに登録する。また、送信先である移動計算機2に対応する鍵で、登録要求に対する応答 packets （登録成功 packets ）のペイロードを暗号化して、これを移動計算機2宛てに返送する。

【0041】なお、図5において、Home-addr

は移動計算機2のホームアドレスを、Current-addrは移動計算機2の現在位置アドレスを、KeyはこのHome-addrとCurrent-addrの組を持つ packets を転送する際に暗号化や復号に用いる鍵であり、転送先ノードに対応して記憶される。

【0042】暗号化された応答 packets を受信した移動計算機2では、送信元の packets 中継装置5に対応する鍵で該 packets を復号し、得られた応答 packets から、登録に成功したことを認識する。

【0043】次に、組織外のグローバルネットに移動した場合について説明する。移動計算機2が組織外のグローバルネットに移動した旨の情報がセットされると、Border Gateway IP addressに設定されたアドレスを用いて、組織ネットワーク1の出口の境界ゲートウェイ4のグローバルアドレスインタフェース宛に、対応する鍵で暗号化した移動IPの登録要求 packets を送信する。この packets 形式を図4(a)に示す。ハッチングされた部分は暗号化されている部分である（図4(b)～(f)も同様である）。

【0044】境界ゲートウェイ4は、自分宛に暗号化 packets が送信されてくると、送信元を調べ、送信元（この場合、移動計算機2）に対応する鍵でこの packets を復号し、得られた packets の内容を検査する。packets ・ヘッダ内の識別情報（例えば packets タイプ・フィールドに記述されたコード）から移動IPの登録要求であることが判ると、該 packets から送信元の移動計算機2のホームアドレスと現在位置アドレスとを取り出し、これを図5のような管理テーブルに登録する。

【0045】次に、境界ゲートウェイ4は、転送先であるホームネットワーク11の packets 中継装置5に対応する鍵で該移動登録 packets を再暗号化し、これを該 packets 中継装置5宛てに転送する。この packets 形式を図4(b)に示す。

【0046】ホームネットワーク11の packets 中継装置5は、境界ゲートウェイ4からの中継/再暗号化された登録要求 packets を受け取ると、packets ヘッダから送信元を調べ、（暗号化 packets のヘッダにおける）送信元である境界ゲートウェイ4に対応する鍵でこの packets を復号し、得られた packets の内容を検査する。packets ・ヘッダ内の識別情報から移動IPの登録要求であることが判ると、該 packets から送信元の移動計算機2のホームアドレスと現在位置アドレスとを取り出し、これを図5のような管理テーブルに登録する。

【0047】また、packets 中継装置5は、移動計算機2に登録要求に対する応答 packets （登録成功 packets ）を返送するために、次段ノード（中継ノード）となる境界ゲートウェイ4宛てに、これに対応する鍵で暗号化した該応答 packets を送信する。この packets 形式を図4(c)に示す。

【0048】境界ゲートウェイ4は、packets 中継装置



15

5からの暗号化パケットを受け取ると、送信元を調べ、送信元すなわちパケット中継装置5に対応する鍵でこのパケットを復号し、得られたパケットの内容を検査する。パケット・ヘッダ内の識別情報から移動IPの応答パケットであることが判ると、パケット・ヘッダ内に記述された移動計算機2のホームアドレスと、図5の管理テーブルとから、移動計算機2の現在位置アドレスを求め、移動計算機2に対応する鍵で再暗号化した応答パケットを、この移動計算機2の現在位置アドレス宛てに転送する。このパケット形式を図4(d)に示す。

【0049】暗号化された応答パケットを受信した移動計算機2では、(暗号化パケットのヘッダにおける)送信元である境界ゲートウェイ4に対応する鍵で該パケットを復号し、得られた応答パケットから、登録に成功したことを認識する。

【0050】以上のように、移動IPの登録要求パケットが受諾されると、それ以降、移動計算機2のホームアドレス宛に送信されてきたパケットをホームネットワーク11のパケット中継装置5が捕捉し、これを移動計算機2の現在位置アドレス宛パケット内にカプセル化し、さらにこれを境界ゲートウェイ2に対応する鍵で暗号化して、境界ゲートウェイ5のプライベートアドレス宛に転送する。このパケット形式を図4(e)に示す。なお、図4(e)ではデータグラム(Data gram)の部分に通信相手宛で移動計算機2のホームアドレス宛のパケットがカプセル化される。そして、境界ゲートウェイ5は前述した移動登録の応答と同様にこのパケットを中継し、移動計算機宛に再暗号化して転送する。このパケット形式を図4(f)に示す。

【0051】また、移動計算機2が通信相手のサーバ7にパケットを送信する場合も、サーバ7のアドレスがホームネットワーク11のパケット中継装置5と同じポリシーで管理されるプライベートアドレスであるなら、前述の登録要求の場合と同様にして、移動計算機2は境界ゲートウェイ4との間で暗号化し、境界ゲートウェイ4のグローバルアドレス宛に送信する。そして、境界ゲートウェイ4は一度これを復号し、サーバ7宛のプライベートアドレスを用いた暗号化パケットに変換して転送する。

【0052】このように、本実施形態に係る境界ゲートウェイ4により、グローバルネットワークとプライベートネットワークの境界で、2つの個別の暗号化転送路を構築することで、2つのアドレス空間を跨ぐ通信を可能とする。

【0053】以上、本実施形態について説明してきたが、従来の移動IP方式では、移動計算機はホームネットワークとの到達可能性(reachability)の保証された単一空間内でのみ移動が許されており、大規模な組織で組織内ネットワークをプライベートアドレスで構築している場合、組織外のグローバルアドレス領

16

域に移動した計算機からは移動IP方式をそのまま使用できなかったが、本実施形態によれば、移動計算機側で自身の現在位置に応じて適切な形式でパケットを生成、送信するような制御を可能とし、また、組織ネットワークの入口で移動計算機からのパケットを一旦受信し、内容を確認して、組織内の該当するホームエージェント

(パケット中継装置)宛に転送する処理を行うことにより、企業ネット等の組織ネットがプライベートアドレスで運用しており、移動計算機が組織外のグローバルアドレスに移動しても移動IP方式をそのまま使用し続けることができる。

【0054】一般に、大規模ネットワークでは、組織ネットの入口で通信内容のログを取ったりすることが多く、境界ゲートウェイの処理のオーバーヘッドは実際には問題にならない場合が多い。また、境界ゲートウェイでファイアウォールなどの他の制御機構を共存させる場合も拡張が容易である。

【0055】また、本実施形態において、インターネットプロバイダなどに接続するシーケンス内で移動計算機のIPネットワーク上の位置を検出することで、移動計算機側の制御をさらに容易にできる。

【0056】なお、本発明は、RFC2002に示される移動IPだけでなく、他の様々な移動通信プロトコルに対しても適用可能である。また、以上の各機能は、ソフトウェアとしても実現可能である。また、上記した各手順あるいは手段をコンピュータに実行させるためのプログラムを記録した機械読取り可能な媒体として実施することもできる。本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【0057】

【発明の効果】本発明によれば、移動計算機が本来属するホームネットワークとは異なるアドレス空間に移動した場合、移動計算機と境界ゲートウェイ等のパケット転送装置との間でそのアドレス空間におけるアドレスを用いて通信を行い、境界ゲートウェイ等のパケット転送装置とホームネットワーク内に位置するホームエージェント等のパケット転送装置やサーバ装置等のノードとの間でホームネットワークにおけるアドレスを用いて通信を行うので、移動計算機が組織外のグローバルアドレスに移動しても移動IP方式をそのまま使用し続けることができる。

【図面の簡単な説明】

【図1】本実施形態に係るネットワークの基本構成を示す図

【図2】制御パネルの一例を示す図

【図3】制御パネルの他の例を示す図

【図4】パケット形式の例を示す図

【図5】管理テーブルの一例を示す図

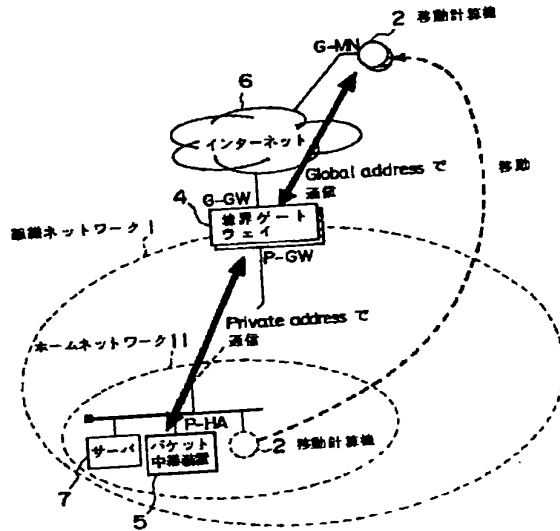
【図6】移動IP方式について説明するための図

## 【符号の説明】

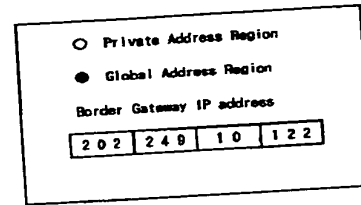
- 1…組織ネットワーク  
2…移動計算機  
5…パケット中継装置

- \* 6…インターネット  
4…境界ゲートウェイ  
7…サーバ  
\* 11…ホームネットワーク

【図 1】



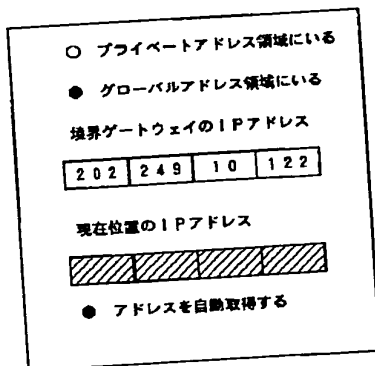
【図 2】



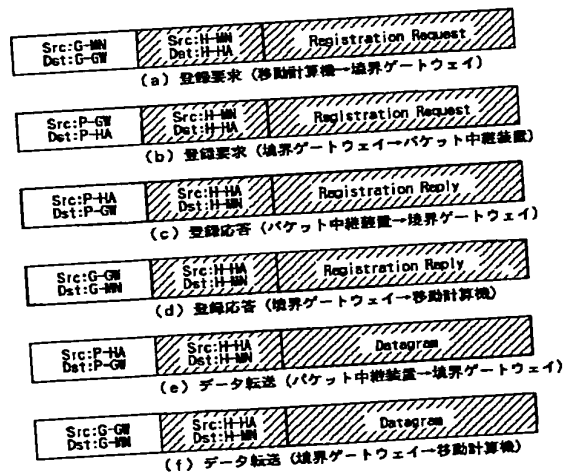
【図 5】

Home-addr	Current-addr	Keys

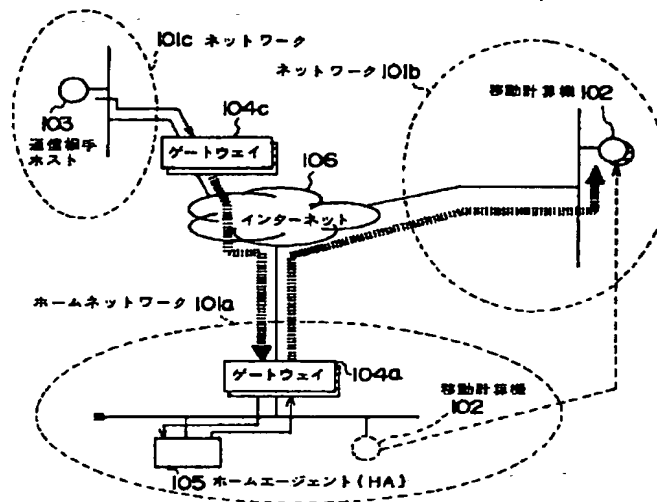
【図 3】



【図 4】



【図 6】



## 【手続補正書】

【提出日】平成 10 年 10 月 7 日

## 【手続補正 1】

【補正対象書類名】明細書

【補正対象項目名】全文

【補正方法】変更

【補正内容】

【書類名】明細書

【発明の名称】 パケット中継装置、移動計算機装置、移動計算機管理装置、パケット中継方法、パケット送信方法及び移動計算機位置登録方法

## 【特許請求の範囲】

【請求項 1】 移動計算機がネットワーク間を移動して通信を行えるようにサポートするネットワークシステム中に設置され、移動計算機のアドレスが送信元もしくは宛先に付されたパケットを中継するパケット中継装置であって、

ホームネットワークとは異なるアドレス方式で管理される移動先ネットワークから、位置登録のために移動計算機が発したパケットであって、ホームネットワークとは異なるアドレスを用いる形式のものを受信する受信手段と、

受信した前記パケットの内容を検査し、この内容に基づいて、該パケットを、プライベートアドレス形式で管理される、移動計算機のホームネットワークに設置された通信相手の計算機へ、プライベートアドレスを用いる形式として転送する転送手段とを具備することを特徴とするパケット中継装置。

【請求項 2】 前記受信手段は、受信した前記パケット

を、前記移動計算機との間で使用される鍵を用いて復号する手段を含み、

前記転送手段は、復号されたパケットを、前記通信相手の計算機との間で使用される鍵を用いて再度暗号化し、暗号化されたパケットに、送信元を自装置のプライベートアドレスとし、宛先を前記通信相手のプライベートアドレスとするヘッダを付加する手段を含むことを特徴とする請求項 1 に記載のパケット中継装置。

【請求項 3】 自装置のプライベートアドレスと、ホームネットワークとは異なるアドレスとしてグローバルアドレスとを記憶する第 1 の記憶手段と、

前記移動計算機の、移動先ネットワークにおける現在位置アドレス、ホームネットワークにおけるホームアドレス、及び前記移動計算機との間での暗号化に使用される鍵を記憶する第 2 の記憶手段とを更に具備することを特徴とする請求項 1 に記載のパケット中継装置。

【請求項 4】 前記通信相手の計算機が、前記移動計算機宛のパケットを該移動計算機の現在位置アドレス宛に転送する手段を有する移動計算機管理装置であり、受信した前記パケットが該現在位置アドレスの情報を含む位置登録要求パケットである場合に、該現在位置アドレスを前記第 2 の記憶手段に登録する手段を更に具備することを特徴とする請求項 3 に記載のパケット中継装置。

【請求項 5】 前記受信手段は、前記通信相手の計算機から、プライベートアドレスを用いる形式の別のパケットを受信する手段を含み、

前記転送手段は、受信した前記別のパケットの内容を検査し、この内容に基づいて、該別のパケットを、移動先

ネットワークの前記移動計算機へ、ホームネットワークとは異なるアドレスを用いる形式として転送する手段を含むことを特徴とする請求項 1 に記載の packets 中継装置。

【請求項 6】前記受信手段は、受信した前記別の packets を、前記通信相手の計算機との間で使用される鍵を用いて復号する手段を含み、

前記転送手段は、復号された packets を、前記移動計算機との間で使用される鍵を用いて再度暗号化し、暗号化された packets に、送信元を自装置のグローバルアドレスとし、宛先を前記移動計算機のグローバルアドレスとするヘッダを付加する手段を含むことを特徴とする請求項 5 に記載の packets 中継装置。

【請求項 7】相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置であって、自装置宛の packets を自装置の現在位置アドレス宛に転送する手段を有する移動計算機管理装置の設置されたホームネットワークと同じプライベートアドレス空間に自装置が接続されているか否かを示す情報を記憶する第 1 の記憶手段と、

前記ホームネットワークのプライベートアドレス空間と、これとは異なるアドレス空間との境界に設置され、該プライベートアドレス空間に接続された計算機と該異なるアドレス空間に接続された計算機との間で送受信される packets を中継する手段を有する packets 中継装置の、該異なるアドレス空間におけるアドレスを記憶する第 2 の記憶手段と、

前記第 1 の記憶手段に記憶された情報が、自装置が前記ホームネットワークとは異なるアドレス空間に接続されていることを示している場合に、現在位置アドレス情報を含む前記移動計算機管理装置宛の位置登録要求 packets を、前記第 2 の記憶手段に記憶された前記 packets 中継装置の異なるアドレス空間におけるアドレスを用いて、送信する送信手段とを具備することを特徴とする移動計算機装置。

【請求項 8】前記送信手段は、前記第 1 の記憶手段に記憶された情報が、自装置が前記ホームネットワークとは異なるアドレス空間に接続されていることを示している場合に、前記ホームネットワークに設置された通信相手の計算機を宛先とする全 packets を暗号化して、前記第 2 の記憶手段に記憶された前記 packets 中継装置の異なるアドレス空間におけるアドレスを用いて、送信する手段を含むことを特徴とする請求項 7 に記載の移動計算機装置。

【請求項 9】移動先ネットワークにおけるアドレスを自動取得するか否かを設定する手段と、前記第 1 の記憶手段に記憶された情報が、自装置が前記ホームネットワークとは異なるアドレス空間に接続されていることを示している場合に、前記自動取得することを示す設定がされているならば、該異なるアドレス空間

におけるアドレスの割り当てを受けるべく所定のプロトコルを実行して取得したアドレスを自装置の現在位置アドレスとする手段とを更に具備することを特徴とする請求項 7 に記載の移動計算機管理装置。

【請求項 10】移動計算機がネットワーク間を移動して通信を行えるように、該移動計算機のホームネットワーク内に設置され、該移動計算機宛の packets を該移動計算機の現在位置アドレス宛に転送する手段を有する移動計算機管理装置であって、

前記ホームネットワークにおける各移動計算機のホームアドレス情報と、各移動計算機がホームネットワーク外に移動した場合の現在位置アドレス情報とを対応付けて記憶する記憶手段と、

前記ホームネットワークのプライベートアドレス空間と、これとは異なるアドレス空間との境界に設置され、該プライベートアドレス空間に接続された計算機と該異なるアドレス空間に接続された計算機との間で送受信される packets を中継する手段を有する packets 中継装置から中継されてきた暗号化 packets を復号し、得られた packets が自装置の管理対象である移動計算機から自装置宛に発せられた、現在位置アドレス情報を含む位置登録 packets である場合に、該現在位置アドレス情報を前記記憶手段に登録する手段とを具備することを特徴とする移動計算機管理装置。

【請求項 11】前記位置登録 packets に対する前記移動計算機宛の登録応答 packets を、前記 packets 中継装置宛に暗号化して送信する手段を更に具備することを特徴とする請求項 10 に記載の移動計算機管理装置。

【請求項 12】前記ホームネットワーク外に移動中の移動計算機のホームアドレス宛に転送されてきた packets を捕捉した場合、該 packets を、送信元を自装置のアドレス、宛先を該移動計算機の現在位置アドレスとする packets にカプセル化し、このカプセル化された packets を暗号化して、前記 packets 中継装置の前記プライベートアドレス空間におけるアドレスを用いて、送信する手段を更に具備することを特徴とする請求項 10 に記載の移動計算機管理装置。

【請求項 13】移動計算機がネットワーク間を移動して通信を行えるようにサポートするネットワークシステム中に設置され、移動計算機のアドレスが送信元もしくは宛先に付された packets を中継する packets 中継装置の packets 中継方法であって、ホームネットワークとは異なるアドレス方式で管理される移動先ネットワークから、位置登録のために移動計算機が発した packets であって、ホームネットワークとは異なるアドレスを用いる形式のものを受信し、受信した前記 packets の内容を検査し、この内容に基づいて、該 packets を、プライベートアドレス形式で管理される、移動計算機のホームネットワークに設置される通信相手の計算機へ、プライベートアドレスを用いる形

式として転送することを特徴とするパケット中継方法。

【請求項 14】相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置のパケット送信方法であって、

自装置宛のパケットを自装置の現在位置アドレス宛に転送する手段を有する移動計算機管理装置の設置されたホームネットワークと同じプライベートアドレス空間に自装置が接続されているか否かを示す情報を得て、これを第 1 の記憶手段に記憶し、該ホームネットワークのプライベートアドレス空間と、これとは異なるアドレス空間との境界に設置され、該プライベートアドレス空間に接続された計算機と該異なるアドレス空間に接続された計算機との間で送受信されるパケットを中継する手段を有するパケット中継装置の、該異なるアドレス空間におけるアドレスを得た場合に、これを第 2 の記憶手段に記憶し、

前記第 1 の記憶手段に記憶された情報が、自装置が前記ホームネットワークとは異なるアドレス空間に接続されていることを示している場合に、現在位置アドレス情報を含む前記移動計算機管理装置宛の位置登録要求パケットを、前記第 2 の記憶手段に記憶された前記パケット中継装置の異なるアドレス空間におけるアドレスを用いて、送信することを特徴とするパケット送信方法。

【請求項 15】移動計算機がネットワーク間を移動して通信を行えるように、該移動計算機のホームネットワーク内に設置され、該移動計算機宛のパケットを該移動計算機の現在位置アドレス宛に転送する手段を有する移動計算機管理装置の移動計算機位置登録方法であって、前記ホームネットワークのプライベートアドレス空間と、これとは異なるアドレス空間との境界に設置され、該プライベートアドレス空間に接続された計算機と該異なるアドレス空間に接続された計算機との間で送受信されるパケットを中継する手段を有するパケット中継装置から中継されてきた暗号化パケットを復号し、得られたパケットが自装置の管理対象である移動計算機から自装置宛に発せられた、現在位置アドレス情報を含む位置登録パケットである場合に、該現在位置アドレス情報を該移動計算機のホームアドレス情報に対応付けて記憶することを特徴とする移動計算機位置登録方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、相互接続している複数のネットワーク上を移動しながら通信を行う移動計算機及びその移動計算機を宛先または送信元とするデータパケットを中継するパケット中継装置並びにパケット中継方法、パケット送信方法及び移動計算機登録方法に関する。

【0002】

【従来の技術】計算機システムの小型化、低価格化やネットワーク環境の充実に伴って、計算機システムの利用

は急速にかつ種々の分野に広く拡大し、また集中型システムから分散型システムへの移行が進んでいる。特に近年では計算機システム自体の進歩、能力向上に加え、コンピュータ・ネットワーク技術の発達・普及により、オフィス内のファイルやプリンタなどの資源共有のみならず、オフィス外、一組織外とのコミュニケーション（電子メール、電子ニュース、ファイルの転送など）が可能になり、これらが広く利用されはじめた。特に近年では、世界最大のコンピュータネットワーク「インターネット（internet）」の利用が普及しており、インターネットと接続し、公開された情報、サービスを利用したり、逆にインターネットを通してアクセスしてくる外部ユーザに対し、情報、サービスを提供することで、新たなコンピュータビジネスが開拓されている。また、インターネット利用に関して、新たな技術開発、展開がなされている。

【0003】また、このようなネットワークの普及に伴い、移動通信（mobile computing）に対する技術開発も行われている。移動通信では、携帯型の端末、計算機を持ったユーザがネットワーク上を移動して通信する。ときには通信を行いながらネットワーク上の位置を変えていく場合もあり、そのような通信において変化する移動計算機のネットワーク上のアドレスを管理し、正しく通信内容を到達させるための方式が必要である。

【0004】一般に移動通信を行う場合、移動計算機が所属していたネットワークに移動計算機の移動先データを管理するルータ（ホームエージェント）を置き、移動計算機が移動した場合、このホームエージェントに対して現在位置を示す登録メッセージを送る。登録メッセージが受け取られたら、移動計算機宛データの送信はそのホームエージェントを経由して、移動計算機の元のアドレス宛の IP パケットを移動計算機の現在位置アドレス宛パケット内にカプセル化することで移動計算機に対するデータの経路制御が行われる。例えば、図 6 では、元々ホームネットワーク 101a に属していた移動計算機 102 が、他のネットワーク 101b に移動し、ネットワーク 101c 内の他の計算機（CH）103 との間で通信を行う場合に、移動計算機 102 に対しホームエージェント（HA）105 が上記の役割を行う。この方式は、インターネットの標準化団体である IETF の mobile-IP ワーキンググループで標準化が進められている移動 IP と呼ばれる方式である（文献：RFC 2002, IP mobility support (C. Perkins)）。

【0005】また、ネットワークが普及し、ネット間の自由な接続が実現され、膨大なデータ、サービスのやりとりがなされる場合、セキュリティ上の問題を考慮する必要が生じてくる。例えば組織内部の秘密情報の外部ネットワークへの漏洩をいかに防ぐか、という問題や、組

織外からの不正な侵入から、組織内ネットワークに接続された資源、情報をいかに守るか、という問題である。インターネットは、当初学術研究を目的に構築されたため、ネットワークの接続による自由なデータサービスのやりとりを重視しており、このようなセキュリティ上の問題は考慮されていなかったが、近年多くの企業、団体がインターネットに接続するようになり、セキュリティ上の問題から自組織ネットワークを防衛する機構が必要となってきた。

【0006】そこで、インターネット上でデータパケットを交換する際に、外部にデータパケットを送出する前にその内容を暗号化し認証コードをつけ、受信したサイトで認証コードを確認し復号化する、という方法がある。この方法によれば、たとえ組織外のユーザが外部ネットワーク上のデータパケットを取り出しても、内容が暗号化されているので、決してその内部が漏洩することがなく、安全な通信が確保できる。

【0007】このような暗号化通信をサポートするゲートウェイ計算機で守られた（ガードされた）ネットワーク同士であれば相互に暗号化通信が可能であり、また前述の移動計算機が自分でパケットの暗号化、復号を行う機能をサポートしていれば、任意のゲートウェイ間、またはゲートウェイ～移動計算機間で暗号化通信がサポートできる。例えば図6では、元々ホームネットワーク101aに属していた移動計算機102が、他のネットワーク101bに移動し、ネットワーク101c内の他の計算機（CH）103と暗号化、復号機能をサポートするゲートウェイ104a、104cを介して暗号化通信を行う。

【0008】図6では、移動IPとパケット暗号化を併用して通信を行う場合、パケットの転送経路は、CH→ゲートウェイ104c→ゲートウェイ104a→ホームエージェント（HA）105→ゲートウェイ104a→移動計算機102となり、ゲートウェイ104aでは、一旦パケットは復号されてホームエージェント105に送られ、その後、再度ホームエージェント105発のパケットが暗号化される。

【0009】さて、移動IP方式では、単一のアドレス空間上を移動計算機が移動する場合のみを想定して、プロトコルが構成されている。すなわち、移動先からの現在位置の登録メッセージは必ずホームネットのホームエージェントに到達可能であると仮定している。しかし、昨今では大規模な組織がインターネットに接続する場合、IPアドレスの枯渇の問題から、組織内の全てのホストにグローバルIPアドレスが割り当てられているのは稀で、組織内はプライベートアドレス（文献：RFC1597）で運用し、外部に通信する場合は、グローバルアドレスへのアドレス変換を行う場合が多い。

【0010】その場合、グローバルアドレス領域に移動

した移動計算機から、プライベートアドレス領域内のホームエージェントに送信された登録要求パケットは、そのままでは到達可能でない。

【0011】

【発明が解決しようとする課題】従来の移動IP方式では、移動計算機はホームネットワークとの到達可能性（reachability）を仮定してプロトコルを構成していたため、ホームネットワークと共通のアドレス空間内のみを移動するという制約があった。このため、組織がプライベートアドレスで運用された場合、移動計算機が組織ネットワークの外（グローバルアドレス領域）に移動すると、移動IP方式がそのまま使用できないという欠点があった。

【0012】本発明は、上記事情を考慮してなされたもので、複数の計算機が複数の相互接続された通信ネットワークにより互いに接続されて相互に通信可能に構成された計算機システムで、移動IPによる移動計算機への自動経路制御がサポートされている場合において、ホームネットワークと異なるアドレス管理領域に移動した移動計算機発の位置登録メッセージなどのパケットの適切な処理を可能とするパケット中継装置、移動計算機装置、移動計算機管理装置、パケット中継方法、パケット送信方法及び移動計算機位置登録方法を提供することを目的とする。

【0013】

【課題を解決するための手段】本発明（請求項1）は、移動計算機がネットワーク間を移動して通信を行えるようにサポートするネットワークシステム中に設置され、移動計算機のアドレスが送信元もしくは宛先に付されたパケットを中継するパケット中継装置であって、ホームネットワークとは異なるアドレス（例えばグローバルアドレス）方式で管理される移動先ネットワークから、位置登録のために移動計算機が発したパケットであって、ホームネットワークとは異なるアドレスを用いる形式のものを受信する受信手段と、受信した前記パケットの内容を検査し、この内容に基づいて、該パケットを、プライベートアドレス形式で管理される、移動計算機のホームネットワークに設置された通信相手の計算機へ、プライベートアドレスを用いる形式として転送する転送手段とを具備することを特徴とする。

【0014】なお、発明の実施の形態においては、パケット中継装置を「境界ゲートウェイ」と呼ぶことがある。好ましくは、前記受信手段は、受信した前記パケットを、前記移動計算機との間で使用される鍵を用いて復号する手段を含み、前記転送手段は、復号されたパケットを、前記通信相手の計算機との間で使用される鍵を用いて再度暗号化し、暗号化されたパケットに、送信元を自装置のプライベートアドレスとし、宛先を前記通信相手のプライベートアドレスとするヘッダを付加する手段を含むようにしてもよい。

【0015】このましくは、自装置のプライベートアドレスと、ホームネットワークとは異なるアドレスとしてグローバルアドレスとを記憶する第1の記憶手段と、前記移動計算機の、移動先ネットワークにおける現在位置アドレス、ホームネットワークにおけるホームアドレス、及び前記移動計算機との間での暗号化に使用される鍵を記憶する第2の記憶手段とを更に具備するようにしてもよい。

【0016】好ましくは、前記通信相手の計算機が、前記移動計算機宛のパケットを該移動計算機の現在位置アドレス宛に転送する手段を有する移動計算機管理装置であり、受信した前記パケットが該現在位置アドレスの情報を含む位置登録要求パケットである場合に、該現在位置アドレスを前記第2の記憶手段に登録する手段を更に具備するようにしてもよい。

【0017】好ましくは、前記受信手段は、前記通信相手の計算機から、プライベートアドレスを用いる形式の別のパケットを受信する手段を含み、前記転送手段は、受信した前記別のパケットの内容を検査し、この内容に基づいて、該別のパケットを、移動先ネットワークの前記移動計算機へ、ホームネットワークとは異なるアドレスを用いる形式として転送する手段を含むようにしてもよい。

【0018】好ましくは、前記受信手段は、受信した前記別のパケットを、前記通信相手の計算機との間で使用される鍵を用いて復号する手段を含み、前記転送手段は、復号されたパケットを、前記移動計算機との間で使用される鍵を用いて再度暗号化し、暗号化されたパケットに、送信元を自装置のグローバルアドレスとし、宛先を前記移動計算機のグローバルアドレスとするヘッダを付加する手段を含むようにしてもよい。

【0019】本発明（請求項7）は、相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機管理装置であって、自装置宛のパケットを自装置の現在位置アドレス宛に転送する手段を有する移動計算機管理装置の設置されたホームネットワークと同じプライベートアドレス空間に自装置が接続されているか否かを示す情報を記憶する第1の記憶手段と、前記ホームネットワークのプライベートアドレス空間と、これとは異なるアドレス空間との境界に設置され、該プライベートアドレス空間に接続された計算機と該異なるアドレス空間に接続された計算機との間で送受信されるパケットを中継する手段を有するパケット中継装置の、該異なるアドレス空間におけるアドレスを記憶する第2の記憶手段と、前記第1の記憶手段に記憶された情報が、自装置が前記ホームネットワークとは異なるアドレス空間に接続されていることを示している場合に、現在位置アドレス情報を含む前記移動計算機管理装置宛の位置登録要求パケットを、前記第2の記憶手段に記憶された前記パケット中継装置の異なるアドレス空間におけるアドレスを用い

て、送信する送信手段とを具備することを特徴とする。

【0020】好ましくは、前記送信手段は、前記第1の記憶手段に記憶された情報が、自装置が前記ホームネットワークとは異なるアドレス空間に接続されていることを示している場合に、前記ホームネットワークに設置された通信相手の計算機を宛先とする全パケットを暗号化して、前記第2の記憶手段に記憶された前記パケット中継装置の異なるアドレス空間におけるアドレスを用いて、送信する手段を含むようにしてもよい。

【0021】好ましくは、移動先ネットワークにおけるアドレスを自動取得するか否かを設定する手段と、前記第1の記憶手段に記憶された情報が、自装置が前記ホームネットワークとは異なるアドレス空間に接続されていることを示している場合に、前記自動取得することを示す設定がされているならば、該異なるアドレス空間におけるアドレスの割り当てを受けるべく所定のプロトコルを実行して取得したアドレスを自装置の現在位置アドレスとする手段とを更に具備するようにしてもよい。

【0022】本発明（請求項10）は、移動計算機がネットワーク間を移動して通信を行えるように、該移動計算機のホームネットワーク内に設置され、該移動計算機宛のパケットを該移動計算機の現在位置アドレス宛に転送する手段を有する移動計算機管理装置であって、前記ホームネットワークにおける各移動計算機のホームアドレス情報と、各移動計算機がホームネットワーク外に移動した場合の現在位置アドレス情報とを対応付けて記憶する記憶手段と、前記ホームネットワークのプライベートアドレス空間と、これとは異なるアドレス空間との境界に設置され、該プライベートアドレス空間に接続された計算機と該異なるアドレス空間に接続された計算機との間で送受信されるパケットを中継する手段を有するパケット中継装置から中継されてきた暗号化パケットを復号し、得られたパケットが自装置の管理対象である移動計算機から自装置宛に発せられた、現在位置アドレス情報を含む位置登録パケットである場合に、該現在位置アドレス情報を前記記憶手段に登録する手段とを具備することを特徴とする。

【0023】なお、発明の実施の形態においては、移動計算機管理装置を「パケット中継装置」もしくは「ホームエージェント」と呼ぶことがある。好ましくは、前記位置登録パケットに対する前記移動計算機宛の登録応答パケットを、前記パケット中継装置宛に暗号化して送信する手段を更に具備するようにしてもよい。

【0024】好ましくは、前記ホームネットワーク外に移動中の移動計算機のホームアドレス宛に転送されてきたパケットを捕捉した場合、該パケットを、送信元を自装置のアドレス、宛先を該移動計算機の現在位置アドレスとするパケットにカプセル化し、このカプセル化されたパケットを暗号化して、前記パケット中継装置の前記プライベートアドレス空間におけるアドレスを用いて、

送信する手段を更に具備するようにしてもよい。

【0025】本発明（請求項13）は、移動計算機がネットワーク間を移動して通信を行えるようにサポートするネットワークシステム中に設置され、移動計算機のアドレスが送信元もしくは宛先に付されたパケットを中継するパケット中継装置のパケット中継方法であって、ホームネットワークとは異なるアドレス（例えばグローバルアドレス）方式で管理される移動先ネットワークから、位置登録のために移動計算機が発したパケットであって、ホームネットワークとは異なるアドレスを用いる形式のものを受信し、受信した前記パケットの内容を検査し、この内容に基づいて、該パケットを、プライベートアドレス形式で管理される、移動計算機のホームネットワークに設置された通信相手の計算機へ、プライベートアドレスを用いる形式として転送することを特徴とする。

【0026】本発明（請求項14）は、相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置のパケット送信方法であって、自装置宛のパケットを自装置の現在位置アドレス宛に転送する手段を有する移動計算機管理装置の設置されたホームネットワークと同じプライベートアドレス空間に自装置が接続されているか否かを示す情報を得て、これを第1の記憶されているか否かを示す情報を得て、これを第1の記憶手段に記憶し、該ホームネットワークのプライベートアドレス空間と、これとは異なるアドレス空間との境界に設置され、該プライベートアドレス空間に接続された計算機と該異なるアドレス空間に接続された計算機との間で送受信されるパケットを中継する手段を有するパケット中継装置の、該異なるアドレス空間におけるアドレスを得た場合に、これを第2の記憶手段に記憶し、前記第1の記憶手段に記憶された情報が、自装置が前記ホームネットワークとは異なるアドレス空間に接続されていることを示している場合に、現在位置アドレス情報を含む前記移動計算機管理装置宛の位置登録要求パケットを、前記第2の記憶手段に記憶された前記パケット中継装置の異なるアドレス空間におけるアドレスを用いて、送信することを特徴とする。

【0027】なお、第1の記憶手段への記憶と第2の記憶手段への記憶については、第1の記憶手段への記憶が先に行われる場合と、第2の記憶手段への記憶が先に行われる場合とがあり得、上記の記載はその両方の場合を含む意味である。

【0028】本発明（請求項15）は、移動計算機がネットワーク間を移動して通信を行えるように、該移動計算機のホームネットワーク内に設置され、該移動計算機宛のパケットを該移動計算機の現在位置アドレス宛に転送する手段を有する移動計算機管理装置の移動計算機位置登録方法であって、前記ホームネットワークのプライベートアドレス空間と、これとは異なるアドレス空間との境界に設置され、該プライベートアドレス空間に接続

された計算機と該異なるアドレス空間に接続された計算機との間で送受信されるパケットを中継する手段を有するパケット中継装置から中継されてきた暗号化パケットを復号し、得られたパケットが自装置の管理対象である移動計算機から自装置宛に発せられた、現在位置アドレス情報を含む位置登録パケットである場合に、該現在位置アドレス情報を該移動計算機のホームアドレス情報に対応付けて記憶することを特徴とする。

【0029】なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【0030】従来、移動IP方式では、移動計算機はホームネットワークとの到達可能性（reachability）の保証された単一空間内でのみ移動が許されており、例えば大規模な組織で組織内ネットワークをプライベートアドレスで構築している場合、組織外のグローバルアドレス領域に移動した計算機からは移動IP方式をそのまま使用できなかった。これに対して本発明によれば、複数のアドレス空間が混在するネットワーク構成において、移動計算機側で自身の現在位置（プライベートアドレス領域で移動しているのか、組織外アドレス領域に移動したか）に応じて適切な形式で登録要求パケットを生成、送信するような制御を可能とし、また、組織ネットワークの入口で移動計算機から送信された登録要求パケットを一旦受信し、内容を確認して、組織内の該当する移動計算機管理装置（パケット中継装置、ホームエージェント）宛に転送する処理を行う（移動IP方式では、ホームエージェントはサブネットに1つ設置され、組織内に複数のホームエージェントが置かれる可能性もあるため）ことにより、例えば企業ネットがプライベートアドレスで運用しており、移動計算機が組織外のグローバルアドレスに移動しても移動IP方式をそのまま使用し続けることができる。

【0031】一般に、大規模ネットワークでは、企業ネットの入口で通信内容のログを取ったりすることが多く、パケット中継装置（境界ゲートウェイ）の処理のオーバーヘッドは実際には問題にならない場合が多い。また、パケット中継装置（境界ゲートウェイ）でファイアウォールなどの他の制御機構を共存させる場合も拡張が容易である。

【0032】また、本発明において、インターネットプロバイダなどに接続するシーケンス内で移動計算機のIPネットワーク上の位置を検出することで、移動計算機側の制御をさらに容易にできる。



## 【0033】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。図1に、本実施形態に係るネットワークの基本構成を示す。図1では、組織ネットワーク1の中にホームネットワーク11が存在する。組織ネットワーク（例えば企業内ネットワーク）1全体はプライベートアドレスで運用されている。移動計算機2は、本来、ホームネットワーク11に接続されているが、現在は移動して、組織ネットワーク外のグローバルアドレスで運用されている箇所に接続されているとする。

【0034】ホームネットワーク11には、パケット中継装置（移動計算機管理装置）5が設置される。このパケット中継装置（移動計算機管理装置）5は、パケット暗号化の機能と、移動IPのホームエージェントの機能（移動計算機の現在位置を管理し、移動計算機宛に送られてきたパケットをカプセル化して現在位置に転送する機能）とを持っている。

【0035】組織ネットワーク1の出口すなわちインターネット6との境界部分には、境界ゲートウェイ4が設置される。この境界ゲートウェイ4は、2つのインタフェースを持ち、組織外のグローバルアドレス（インターネット側）と組織内のプライベートアドレスの両方を持つ。

【0036】なお、本実施形態ではノード間のデータ転送に暗号化通信を用いるが、このノード間の暗号化通信には、ノード間で共有された該ノード間に固有の共通鍵を用いるものとする。この共通鍵は予めノード間で共有しておくか、あるいは必要時にノード間で鍵共有のための手続きを行う。

【0037】以下では移動計算機2が移動先からホームネットワーク11内のパケット中継装置（移動計算機管理装置）5との間で位置登録に関するやり取りを行う場合とサーバ7と通信する場合を例にとりつつ本実施形態について詳しく説明する。

【0038】移動計算機2側では、自身の接続している現在位置に関する情報を図2に例示する制御パネルで設定する。ここで、Private Address Regionは移動計算機2が同じプライベートアドレス体系で運営される組織ネット内で移動したことを、Global Address Regionは組織ネット外部に出たことを示す。

【0039】Global Address Regionを選択した場合は、Border Gateway IP addressに境界ゲートウェイ4のグローバルアドレスを設定する（例えば、202, 249, 10, 122）。また、自身の現在位置のアドレスを設定する（この設定フィールドは図2においては省略してある）。

【0040】なお、上記では、ユーザが陽に設定を行うようにしたが、例えばインターネットプロバイダーのサ

ーバとPPPで接続する際のネゴシエーションメッセージを基にこれらの情報を自動的に設定することも可能である。すなわち、一般にインターネットプロバイダと電話回線を通じてPPPというプロトコルでIP接続を行う場合、PPPプロトコルの初期セット時にICPというプロトコルで割り当てられるアドレスを決める。そのような場合、移動計算機2側では特定のアドレスを設定できないので、例えば図3のように、「アドレスをISP側から自動的割り当てする」あるいは「アドレスを自動取得する」というような設定ボタンを設け、これを選択する。これを選択した場合、PPPのプロトコルの途上で獲得したIPアドレスがそのまま現在位置アドレスにセットされる。

【0041】次に、図2に例示した制御パネルで（あるいは自動的に）現在位置が設定された場合の位置登録メッセージの送信動作を説明する。まず、プライベートネット内で移動した場合について説明する。

【0042】移動計算機2は、組織内（例えば企業内）のプライベートネット内で移動した旨の情報がセットされると、通常の移動IPの規定通り、ホームネットワーク11のパケット中継装置（移動計算機管理装置）5宛に、対応する鍵で登録要求パケットのペイロードを暗号化して送信する。

【0043】暗号化された登録要求パケットを受信したパケット中継装置（移動計算機管理装置）5では、送信元の移動計算機2に対応する鍵で該パケットを復号し、得られたパケットの内容を検査する。パケット・ヘッダ内の識別情報（例えばパケットタイプ・フィールドに記述されたコード）から移動IPの登録要求であることが判ると、該パケットから該移動計算機2のホームアドレスと現在位置アドレスを取り出し、これを図5のような管理テーブルに登録する。また、送信先である移動計算機2に対応する鍵で、登録要求に対する応答パケット（登録成功パケット）のペイロードを暗号化して、これを移動計算機2宛てに返送する。

【0044】なお、図5において、Home-addrは移動計算機2のホームアドレス、Current-addrは移動計算機2の現在位置アドレス、KeysはこのHome-addrとCurrent-addrの組を持つパケットを転送する際に暗号化や復号に用いる鍵であり、転送先ノードに対応して記憶される。

【0045】暗号化された応答パケットを受信した移動計算機2では、送信元のパケット中継装置（移動計算機管理装置）5に対応する鍵で該パケットを復号し、得られた応答パケットから、登録に成功したことを認識する。

【0046】次に、組織外のグローバルネットに移動した場合について説明する。移動計算機2が組織外のグローバルネットに移動した旨の情報がセットされると、Border Gateway IP addressに

設定されたアドレスを用いて、組織ネットワーク1の出口の境界ゲートウェイ4のグローバルアドレスインタフェース宛に、対応する鍵で暗号化した移動IPの登録要求パケットを送信する。このパケット形式を図4(a)に示す。ハッチングされた部分は暗号化されている部分である(図4(b)~(f)も同様である)。

【0047】境界ゲートウェイ4は、自分宛に暗号化パケットが送信されてくると、送信元を調べ、送信元(この場合、移動計算機2)に対応する鍵でこのパケットを復号し、得られたパケットの内容を検査する。パケット・ヘッダ内の識別情報(例えばパケットタイプ・フィールドに記述されたコード)から移動IPの登録要求であることが判ると、該パケットから送信元の移動計算機2のホームアドレスと現在位置アドレスとを取り出し、これを図5のような管理テーブルに登録する。

【0048】次に、境界ゲートウェイ4は、転送先であるホームネットワーク11のパケット中継装置(移動計算機管理装置)5に対応する鍵で該位置登録パケットを再暗号化し、これを該パケット中継装置(移動計算機管理装置)5宛てに転送する。このパケット形式を図4(b)に示す。

【0049】ホームネットワーク11のパケット中継装置(移動計算機管理装置)5は、境界ゲートウェイ4からの中継/再暗号化された登録要求パケットを受け取ると、パケットヘッダから送信元を調べ、(暗号化パケットのヘッダにおける)送信元である境界ゲートウェイ4に対応する鍵でこのパケットを復号し、得られたパケットの内容を検査する。パケット・ヘッダ内の識別情報から移動IPの登録要求であることが判ると、該パケットから送信元の移動計算機2のホームアドレスと現在位置アドレスとを取り出し、これを図5のような管理テーブルに登録する。

【0050】また、パケット中継装置(移動計算機管理装置)5は、移動計算機2に登録要求に対する応答パケット(登録成功パケット)を返送するために、次段ノード(中継ノード)となる境界ゲートウェイ4宛てに、これに対応する鍵で暗号化した該応答パケットを送信する。このパケット形式を図4(c)に示す。

【0051】境界ゲートウェイ4は、パケット中継装置(移動計算機管理装置)5からの暗号化パケットを受け取ると、送信元を調べ、送信元すなわちパケット中継装置(移動計算機管理装置)5に対応する鍵でこのパケットを復号し、得られたパケットの内容を検査する。パケット・ヘッダ内の識別情報から移動IPの応答パケットであることが判ると、パケット・ヘッダ内に記述された移動計算機2のホームアドレスと、図5の管理テーブルとから、移動計算機2の現在位置アドレスを求め、移動計算機2に対応する鍵で再暗号化した応答パケットを、この移動計算機2の現在位置アドレス宛てに転送する。このパケット形式を図4(d)に示す。

【0052】暗号化された応答パケットを受信した移動計算機2では、(暗号化パケットのヘッダにおける)送信元である境界ゲートウェイ4に対応する鍵で該パケットを復号し、得られた応答パケットから、登録に成功したことを認識する。

【0053】以上のように、移動IPの登録要求パケットが受諾されると、それ以降、移動計算機2のホームアドレス宛に送信されてきたパケットをホームネットワーク11のパケット中継装置(移動計算機管理装置)5が捕捉し、これを移動計算機2の現在位置アドレス宛パケット内にカプセル化し、さらにこれを境界ゲートウェイ4に対応する鍵で暗号化して、境界ゲートウェイ4のプライベートアドレス宛に転送する。このパケット形式を図4(e)に示す。なお、図4(e)ではデータグラム(Data gram)の部分に通信相手宛で移動計算機2のホームアドレス宛のパケットがカプセル化される。そして、境界ゲートウェイ4は前述した位置登録の応答と同様にこのパケットを中継し、移動計算機宛に再暗号化して転送する。このパケット形式を図4(f)に示す。

【0054】また、移動計算機2が通信相手のサーバ7にパケットを送信する場合も、サーバ7のアドレスがホームネットワーク11のパケット中継装置(移動計算機管理装置)5と同じポリシーで管理されるプライベートアドレスであるなら、前述の登録要求の場合と同様にし、移動計算機2は境界ゲートウェイ4対応の鍵で暗号化し、境界ゲートウェイ4のグローバルアドレス宛に送信する。そして、境界ゲートウェイ4は一度これを復号し、サーバ7宛のプライベートアドレスを用いた暗号化パケットに変換して転送する。

【0055】このように、本実施形態に係る境界ゲートウェイ4により、グローバルネットワークとプライベートネットワークの境界で、2つの個別の暗号化転送路を構築することで、2つのアドレス空間を跨ぐ通信を可能とする。

【0056】以上、本実施形態について説明してきたが、従来の移動IP方式では、移動計算機はホームネットワークとの到達可能性(reachability)の保証された単一空間内でのみ移動が許されており、大規模な組織で組織内ネットワークをグローバルアドレス領域で構築している場合、組織外のグローバルアドレス領域に移動した計算機からは移動IP方式をそのまま使用できなかったが、本実施形態によれば、移動計算機側で自身の現在位置に応じて適切な形式でパケットを生成、送信するような制御を可能とし、また、組織ネットワークの入口で移動計算機からのパケットを一旦受信し、内容を確認して、組織内の該当するホームエージェント(パケット中継装置)宛に転送する処理を行うことにより、企業ネット等の組織ネットがプライベートアドレスで運用しており、移動計算機が組織外のグローバルアドレスに移動しても移動IP方式をそのまま使用し続ける

ことができる。

【0057】一般に、大規模ネットワークでは、組織ネットの入口で通信内容のログを取ったりすることが多く、境界ゲートウェイの処理のオーバーヘッドは実際には問題にならない場合が多い。また、境界ゲートウェイでファイアウォールなどの他の制御機構を共存させる場合も拡張が容易である。

【0058】また、本実施形態において、インターネットプロバイダなどに接続するシーケンス内で移動計算機のIPネットワーク上の位置を検出することで、移動計算機側の制御をさらに容易にできる。

【0059】なお、本発明は、RFC2002に示される移動IPだけでなく、他の様々な移動通信プロトコルに対しても適用可能である。また、以上の各機能は、ソフトウェアとしても実現可能である。また、本実施形態は、コンピュータに所定の手順を実行させるための（あるいはコンピュータを所定の手段として機能させるための）、あるいはコンピュータに所定の機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体として実施することもできる。本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【0060】

【発明の効果】本発明によれば、移動計算機が本来属するホームネットワークとは異なるアドレス空間に移動し

た場合、移動計算機と境界ゲートウェイ等のパケット中継装置との間でそのアドレス空間におけるアドレスを用いて通信を行い、境界ゲートウェイ等のパケット中継装置とホームネットワーク内に位置するホームエージェント等の移動計算機管理装置やサーバ装置等のノードとの間でホームネットワークにおけるアドレスを用いて通信を行うので、移動計算機が組織外のグローバルアドレスに移動しても移動IP方式をそのまま使用し続けることができる。

【図面の簡単な説明】

【図1】本実施形態に係るネットワークの基本構成を示す図

【図2】制御パネルの一例を示す図

【図3】制御パネルの他の例を示す図

【図4】パケット形式の例を示す図

【図5】管理テーブルの一例を示す図

【図6】移動IP方式について説明するための図

【符号の説明】

1…組織ネットワーク

2…移動計算機

5…パケット中継装置（移動計算機管理装置）

6…インターネット

4…境界ゲートウェイ

7…サーバ

11…ホームネットワーク

---

フロントページの続き

(72)発明者 津田 悦幸  
神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

THIS PAGE BLANK (USPTO)